

Hellinger volume and number-on-the-forehead communication complexity

Troy Lee* Nikos Leonardos† Michael Saks‡ Fengming Wang§

July 22, 2014

Abstract

Information-theoretic methods have proven to be a very powerful tool in communication complexity, in particular giving an elegant proof of the linear lower bound for the two-party disjointness function, and tight lower bounds on disjointness in the multi-party number-in-the-hand (NIH) model. In this paper, we study the applicability of information theoretic methods to the multi-party number-on-the-forehead model (NOF), where determining the complexity of disjointness remains an important open problem.

There are two basic parts to the NIH disjointness lower bound: a direct sum theorem and a lower bound on the one-bit AND function using a beautiful connection between Hellinger distance and protocols revealed by Bar-Yossef, Jayram, Kumar & Sivakumar [BYJKS04]. Inspired by this connection, we introduce the notion of Hellinger volume. We show that it lower bounds the information cost of multi-party NOF protocols and provide a small toolbox that allows one to manipulate several Hellinger volume terms and lower bound a Hellinger volume when the distributions involved satisfy certain conditions. In doing so, we prove a new upper bound on the difference between the arithmetic mean and the geometric mean in terms of relative entropy. We then apply these new tools to obtain a lower bound on the informational complexity of the AND_k function in the NOF setting. Finally, we discuss the difficulties of proving a direct sum theorem for information cost in the NOF model.

Keywords: communication complexity, informational complexity, Hellinger volume, number-on-the-forehead.

1 Introduction

One of the most important research areas in communication complexity is proving lower bounds in the multi-party number-on-the-forehead (NOF) model. The NOF model was introduced in [CFL83], where it was used to prove lower bounds for

*School of Physics and Mathematical Sciences, Nanyang Technological University and Centre for Quantum Technologies. Supported in part by the Singapore National Research Foundation under NRF RF Award No. NRF-NRFF2013-13 and by a NSF postdoctoral fellowship while at Rutgers University. postdoctoral fellowship. Email: troyjlee@gmail.com.

†Department of Computer Science, Rutgers University, NJ, USA Supported in part by NSF under grant CCF 0832787. Email: nikos.leonardos@gmail.com.

‡Mathematics Department, Rutgers University, NJ, USA Supported in part by NSF under grant CCF 0832787. Email: saks@math.rutgers.edu.

§Department of Computer Science, Rutgers University, NJ, USA Supported in part by NSF under grants CCF 0830133, CCF 0832787, and CCF 1064785. Email: fengming@cs.rutgers.edu.

branching programs. Subsequent papers revealed connections of this model to circuit complexity [BT94, HG90, Nis94, NW91] and proof complexity [BPS05]. In particular, an explicit function which requires super-polylogarithmic complexity in the NOF model with polylogarithmically many players would give an explicit function outside of the circuit complexity class ACC^0 .

Essentially all lower bounds on the general NOF model have been shown using the discrepancy method following [BNS92]. This method has been able to show lower bounds of $\Omega(n/2^k)$ for explicit functions [BNS92, CT93, Raz00, FG05]. For the disjointness function, the plain discrepancy method shows poor bounds and a more sophisticated application of discrepancy is needed known as the generalized discrepancy method [Kla07, Raz03, LS07, She11]. The generalized discrepancy method was initially used to show lower bounds of the form $n^{1/k}/2^{2^k}$ [LS09, CA08] and $2^{\Omega(\sqrt{\log n}/\sqrt{k})-k}$ [BHN09] on the k -player NOF complexity of disjointness. Recent work of Sherstov in [She12] and [She13] improved the lower bounds to $\Omega((n/4^k)^{1/4})$ and $\Omega(\sqrt{n}/2^k)$, respectively. A very recent paper of Rao and Yehudayoff [RY14] gives a simplified proof of the latter lower bound and also gives a nearly tight $\Omega(n/4^k)$ lower bound for deterministic protocols. An upper bound of $O(\log^2(n) + k^2 n/2^k)$ for the disjointness function follows from a beautiful protocol of Grolmusz [Gro94].

In this paper we are interested in how information-theoretic methods might be applied to the NOF model. Information-theoretic methods have been very successful in the number-in-the-hand (NIH) multi-party model, in particular giving tight lower bounds on the disjointness function. The first use of information theory in communication complexity lower bounds can be traced to [Abl96]. In [CSWY01] the notions of information cost and informational complexity were defined explicitly. Building on their work, a very elegant information-theoretic framework for proving lower bounds in NIH communication complexity was established in [BYJKS04].

In [BYJKS04] a proof of the linear lower bound for two-party disjointness was given. The proof has two main stages. In the first stage, a direct-sum theorem for informational complexity is shown, which says that the informational complexity of disjointness, $\text{DISJ}_{n,2}(x, y) = \bigvee_{j=1}^n \text{AND}_2(x_j, y_j)$, is lower bounded by n times the informational complexity of the binary AND_2 function. Although it is not known how to prove such a direct-sum theorem directly for the classical randomized complexity, Bar-Yossef et al. prove it for the informational complexity with respect to a suitable distribution. A crucial property of the distribution is that it is over the zeroes of disjointness. At this point we should point out a remarkable characteristic of the method: even though the information cost of a protocol is analyzed with respect to a distribution over zeroes only, the protocol is required to be correct over all inputs. This requirement is essential in the second stage, where a constant lower bound is proved on the informational complexity of AND_2 . This is achieved using properties of the Hellinger distance for distributions. Bar-Yossef et al. reveal a beautiful connection between Hellinger distance and NIH communication protocols. (More properties of Hellinger distance relative to the NIH model have been established in [Jay09].)

In this work we provide tools for accomplishing the second stage in the NOF model. We introduce the notion of Hellinger volume of $m \geq 2$ distributions and show that it can be useful for proving lower bounds on informational complexity in the NOF model, just as Hellinger distance is useful in the NIH model. However, as we point out in the last section, there are fundamental difficulties in proving a direct-sum theorem for informational complexity in the NOF model. Nevertheless, we believe that Hellinger volume and the related tools we prove, could be useful in

an information-theoretic attack on NOF complexity.

A version of this paper was submitted to a journal in 2011, but the refereeing process has been long delayed. In the meantime there has been some overlapping independent work by Beame, Hopkins, Hrubeš and Rashtchian [BHHR14], including lower bounds for the information complexity of the AND function similar to those we give in Section 5 but for restricted settings, and 0-information protocols in the “randomness on the forehead” model, of the type we give in Section 6 but in a more general setting.

2 Preliminaries and notation

Hellinger volume We introduce the notion of Hellinger volume of m distributions. In the next section we show that it has properties similar in flavor to the ones of Hellinger distance.

Definition 1. *The m -dimensional Hellinger volume of distributions p_1, \dots, p_m over Ω is*

$$h_m(p_1, \dots, p_m) = 1 - \sum_{\omega \in \Omega} \sqrt[m]{p_1(\omega) \cdots p_m(\omega)}.$$

Notice that $h_2(p_1, p_2)$ in the case $m = 2$ is the square of the Hellinger distance between distributions p_1 and p_2 .

The following fact follows from the arithmetic-geometric mean inequality.

Fact 1. *For any distributions p_1, \dots, p_m over Ω , $h_m(p_1, \dots, p_m) \geq 0$.*

Random variables and distributions We consider discrete probability spaces (Ω, ζ) , where Ω is a finite set and ζ is a nonnegative valued function on Ω summing to 1. If $(\Omega_1, \zeta_1), \dots, (\Omega_n, \zeta_n)$ are such spaces, their product is the space (Λ, ν) , where $\Lambda = \Omega_1 \times \cdots \times \Omega_n$ is the Cartesian product of sets, and for $\omega = (\omega_1, \dots, \omega_n) \in \Lambda$, $\nu(\omega) = \prod_{j=1}^n \zeta_j(\omega_j)$. In the case that all of the (Ω_i, ζ_i) are equal to a common space (Ω, ζ) we write $\Lambda = \Omega^n$ and $\nu = \zeta^n$.

We use uppercase for random variables, as in \mathbf{Z}, D , and write in bold those that represent vectors of random variables. For a variable X with range \mathcal{X} that is distributed according to a probability distribution μ , i.e. $\Pr[X = x] = \mu(x)$, we write $X \sim \mu$. If X is uniformly distributed in \mathcal{X} , we write $X \in_R \mathcal{X}$.

Information theory Let X, Y, Z be random variables on a common probability space, taking on values, respectively, from finite sets $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$. Let A be any event. The *entropy* of X , the *conditional entropy of X given A* , and the *conditional entropy of X given Y* are respectively (we use \log for \log_2)

$$\begin{aligned} H(X) &= - \sum_{x \in \mathcal{X}} \Pr[X = x] \cdot \log \Pr[X = x], \\ H(X|A) &= - \sum_{x \in \mathcal{X}} \Pr[X = x | A] \cdot \log \Pr[X = x | A], \\ H(X|Y) &= \sum_{y \in \mathcal{Y}} \Pr[Y = y] \cdot H(X|Y = y). \end{aligned}$$

We will need the following facts about the entropy. (See [CT06, Chapter 2], for proofs and more details.)

Proposition 2. *Let X, Y, Z be random variables.*

1. $H(X) \geq H(X|Y) \geq 0$.
2. If \mathcal{X} is the range of X , then $H(X) \leq \log |\mathcal{X}|$.
3. $H(X, Y) \leq H(X) + H(Y)$ with equality if and only if X and Y are independent. This holds for conditional entropy as well. $H(X, Y|Z) \leq H(X|Z) + H(Y|Z)$ with equality if and only if X and Y are independent given Z .

The *relative entropy* or *divergence* of distributions P and Q over Ω is

$$D(P\|Q) = \sum_{x \in \Omega} P(x) \log \frac{P(x)}{Q(x)}.$$

The *mutual information* between X and Y is

$$I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X).$$

Notation We write $[n] = \{1, 2, \dots, n\}$. For a sequence (a_1, \dots, a_n) we let, for $j \in [n]$, $a_{<j} = (a_1, \dots, a_{j-1})$, and $a^{-j} = (a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_k)$. We will denote subsets of $\{0, 1\}^k$ as follows: $I = \{0, 1\}^k$; for $j \in [k]$, I_j is the set of points in I such that the j -th coordinate is set to zero, i.e. $I_j = \{z \in I \mid z_j = 0\}$; I_{OZ} (resp. I_{EZ}) is the set of points in I with an odd (resp. even) number of zeros.

Communication complexity In this work we will be dealing with the multi-party private-coin randomized number-on-the-forehead communication model, introduced by [CFL83]. There are k players, numbered $1, \dots, k$, trying to compute a function $f : \mathcal{Z} \rightarrow \{0, 1\}$, where $\mathcal{Z} = \mathcal{Z}_1 \times \dots \times \mathcal{Z}_k$. On input $z \in \mathcal{Z}$, player j receives input z_j (conceptually, placed on his forehead), but he has access only to z^{-j} . They wish to determine $f(z)$, by broadcasting messages according to a protocol Π . Let the random variable $\Pi(z)$ denote the transcript of the communication on input z (where the probability is over the random coins of the players) and $\Pi_{\text{out}}(z)$ the outcome of the protocol. We call Π a δ -error protocol for f if, for all z , $\Pr[\Pi_{\text{out}}(z) = f(z)] \geq 1 - \delta$. The *communication cost* of Π is $\max |\Pi(z)|$, where the maximum is over all inputs z and over all coin tosses of the players. The δ -error randomized communication complexity of f , denoted $R_\delta(f)$, is the cost of the best δ -error protocol for f . (See [KN06] for more details.)

Communication complexity lower bounds via information theory The informational complexity paradigm, introduced by [CSWY01], and used in [SS02, BYJKS02, CKS03, BYJKS04, JKS03], provides a way to prove lower bounds on communication complexity via information theory. We are given a k -party function f and we want to show that any δ -error randomized NOF protocol Π for f requires high communication. We introduce a probability distribution over the inputs to the players. We then analyze the behavior of Π when run on inputs chosen randomly according to the distribution. The informational complexity is the mutual information of the string of communicated bits (the *transcript* of Π) with the inputs, and provides a lower bound on the amount of communication.

More precisely, let $\Omega = (\Omega, \zeta)$ be a probability space over which are defined random variables $\mathbf{Z} = (Z_1, \dots, Z_k)$ representing the inputs. The *information cost*

of a protocol Π with respect to ζ is defined to be $I(\mathbf{Z}; \Pi(\mathbf{Z}))$, where $\Pi(\mathbf{Z})$ is a random variable following the distribution of the communication transcripts when the protocol Π runs on input $\mathbf{Z} \sim \zeta$. The δ -error informational complexity of f with respect to ζ , denoted $\text{IC}_{\zeta, \delta}(f)$, is $\min_{\Pi} I(\mathbf{Z}; \Pi(\mathbf{Z}))$, where the minimum is over all δ -error randomized NOF protocols for f . The relevance of informational complexity comes from the following proposition.

Proposition 3. $R_{\delta}(f) \geq \text{IC}_{\zeta, \delta}(f)$.

Proof. For any protocol Π , $\text{IC}_{\zeta, \delta}(f) \leq I(\mathbf{X}, \mathbf{Y}; \Pi(\mathbf{X}, \mathbf{Y})) = H(\Pi(\mathbf{X}, \mathbf{Y})) - H(\Pi(\mathbf{X}, \mathbf{Y}) | \mathbf{X}, \mathbf{Y})$. Applying in turn parts (1) and (2) of Proposition 2 gives $\text{IC}_{\zeta, \delta}(f) \leq H(\Pi(\mathbf{X}, \mathbf{Y})) \leq R_{\delta}(f)$. \square

For a collection of distributions $\eta = \{\zeta_1, \dots, \zeta_k\}$, we define the δ -error informational complexity of f with respect to η , denoted $\text{IC}_{\eta, \delta}(f)$, to be $\mathbf{E}_j[\text{IC}_{\zeta_j, \delta}(f)]$, where j is uniformly distributed over $[k]$.

Remark This definition of information cost as an average, is equivalent to the (standard) conditional information cost. We choose this definition, because we think it makes the exposition cleaner.

3 An upper bound on the difference between the arithmetic and geometric mean.

For a nonnegative real sequence $\alpha = (\alpha_1, \dots, \alpha_m)$, let $A(\alpha)$ and $G(\alpha)$ denote its arithmetic and geometric mean respectively. That is

$$A(\alpha) = \frac{1}{m} \sum \alpha_j \quad \text{and} \quad G(\alpha) = \sqrt[m]{\prod \alpha_j}.$$

Theorem 1. For any distribution p over $[m]$,

$$A(p) - G(p) \leq \ln 2 \cdot D(p \| u),$$

where u is the uniform distribution over $[m]$.

Proof. Let $x_j = mp(j)$, $x = (x_1, \dots, x_m)$, and define

$$f(x) = \sum x_j \ln x_j + \sqrt[m]{\prod x_j}.$$

Theorem 1 is equivalent to showing that, for $x_1, \dots, x_m \geq 0$, if $\sum x_j = m$, then $f(x) \geq 1$.

We proceed using Lagrange multipliers. We first need to check that $f(x) \geq 1$ when x is on the boundary, i.e. $x_j = 0$ for some $j \in [m]$. Without loss of generality, assume $x_1 = 0$. By the convexity of $t \ln t$, the minimum is attained when $x_2 = \dots = x_m = m/(m-1)$. Thus,

$$f(x) \geq (m-1) \frac{m}{m-1} \ln \frac{m}{m-1} > m \left(1 - \frac{m-1}{m} \right) = 1.$$

According to [Lue03, Theorem on page 300], it suffices to show that $f(x) \geq 1$ for any x that satisfies the following system of equations.

$$\partial f / \partial x_j = 1 + \ln x_j + \sigma / (m x_j) = \lambda, \quad \text{for } j \in [m], \quad (L)$$

where $\sigma = \sqrt[m]{x_1 \cdots x_m} \neq 0$. Without loss of generality, since $\sum x_j = m$, we may assume $x_m \leq 1$. The system (L) implies

$$\begin{aligned} \sum_{j=1}^{m-1} x_j (\partial f / \partial x_j) &= m - x_m + \sum_{j=1}^{m-1} x_j \ln x_j + \sigma(m-1)/m = \lambda(m - x_m), \\ (m-1)x_m (\partial f / \partial x_m) &= (m-1)(x_m + x_m \ln x_m + \sigma/m) = (m-1)\lambda x_m. \end{aligned}$$

Subtracting the second from the first we get

$$\sum_{j=1}^{m-1} x_j \ln x_j - (m-1)x_m \ln x_m = m(\lambda - 1)(1 - x_m).$$

We also have

$$\sum x_j (\partial f / \partial x_j) = m + f(x) = m\lambda.$$

Suppose $x = (x_1, \dots, x_m)$ satisfies the system (L). Since $x_m \leq 1$, we have $x_m \ln x_m \leq 0$, and using the last two equations we have

$$f(x) = m(\lambda - 1) \geq \frac{\sum_{j=1}^{m-1} x_j \ln x_j}{1 - x_m} \geq \frac{\sum_{j=1}^{m-1} x_j (1 - 1/x_j)}{1 - x_m} = 1.$$

This completes the proof. \square

Corollary 2. For any nonnegative real sequence $\alpha = (\alpha_1, \dots, \alpha_m)$,

$$A(\alpha) - G(\alpha) \leq \sum \alpha_j \ln \frac{\alpha_j}{A(\alpha)}.$$

Proof. Apply Theorem 1 with $p(j) = \alpha_j / \sum \alpha_j$. \square

Remark Let $\hat{\alpha}$ to be a normalized version of α , with $\hat{\alpha}_j = \alpha_j / \sum \alpha_j$. Let also u denote the uniform distribution on $[m]$. Then, the right-hand side takes the form $\sum \alpha_j \ln(m\hat{\alpha}_j) = mA(\alpha) \sum \hat{\alpha}_j \ln(\hat{\alpha}_j / u_j)$, and the above inequality becomes

$$\frac{A(\alpha) - G(\alpha)}{A(\alpha)} \leq m \ln 2 \cdot D(\hat{\alpha} \| u).$$

4 Properties of Hellinger volume

Hellinger volume lower bounds mutual information The next lemma shows that Hellinger volume can be used to lower bound mutual information.

Lemma 3. Consider random variables $Z \in_R [m]$, $\Phi(Z) \in \Omega$, and distributions Φ_z , for $z \in [m]$, over Ω . Suppose that given $Z = z$, the distribution of $\Phi(Z)$ is Φ_z . Then

$$I(Z; \Phi(Z)) \geq \frac{h_m(\Phi_1, \dots, \Phi_m)}{m \ln 2}.$$

Proof. The left-hand side can be expressed as follows (see [CT06, page 20]),

$$\begin{aligned} I(Z; \Phi(Z)) &= \sum_{j, \omega} \Pr[Z = j] \cdot \Pr[\Phi(Z) = \omega | Z = j] \cdot \log \frac{\Pr[\Phi(Z) = \omega | Z = j]}{\Pr[\Phi(Z) = \omega]} \\ &= \sum_{j, \omega} \frac{1}{m} \Phi_j(\omega) \log \frac{\Phi_j(\omega)}{\frac{1}{m} \sum_j \Phi_j(\omega)}, \end{aligned}$$

and the right-hand side

$$h_m(\Phi_1, \dots, \Phi_m) = \sum_{\omega} \left(\frac{1}{m} \sum_j \Phi_j(\omega) - \left(\prod_j \Phi_j(\omega) \right)^{\frac{1}{m}} \right).$$

It suffices to show that for each $\omega \in \Omega$,

$$\sum_j \frac{1}{m} \Phi_j(\omega) \log \frac{\Phi_j(\omega)}{\frac{1}{m} \sum_j \Phi_j(\omega)} \geq \frac{1}{m \ln 2} \left(\frac{1}{m} \sum_j \Phi_j(\omega) - \left(\prod_j \Phi_j(\omega) \right)^{\frac{1}{m}} \right).$$

Let $s = \sum_j \Phi_j(\omega)$, and $\rho(j) = \Phi_j(\omega)/s$, for $j \in [m]$; thus, for all j , $\rho(j) \in [0, 1]$, and $\sum_j \rho(j) = 1$. Under this renaming of variables, the left-hand side becomes $\ln 2 \cdot \frac{s}{m} \sum_j \rho(j) \log(m\rho(j))$ and the right one $\frac{s}{m} \cdot \left(\frac{1}{m} - \sqrt[m]{\prod \rho(j)} \right)$. Thus, we need to show

$$\ln 2 \cdot \sum_j \rho(j) \log(m\rho(j)) \geq \frac{1}{m} - \left(\prod_j \rho(j) \right)^{\frac{1}{m}}.$$

Observe that the left-hand side is $\ln 2 \cdot D(\rho \| u)$, and the inequality holds by Theorem 1. \square

Symmetric-difference lemma Let $P = \{P_z\}_{z \in Z}$ be a collection of distributions over a common space Ω . For $A \subseteq Z$, the *Hellinger volume of A with respect to P* , denoted by $\psi(P; A)$, is

$$\psi(A; P) = 1 - \sum_{\omega \in \Omega} \left(\prod_{z \in A} P_z(\omega) \right)^{1/|A|}.$$

The collection P will be understood from the context and we'll say that the Hellinger volume of A is $\psi(A)$. Note that, from Fact 1, $\psi(A; P) \geq 0$.

The following lemma can be seen as an analog to the weak triangle inequality that is satisfied by the square of the Hellinger distance.

Lemma 4 (Symmetric-difference lemma). *If A, B satisfy $|A| = |B| = |A \Delta B|$, where $A \Delta B = (A \setminus B) \cup (B \setminus A)$. Then*

$$\psi(A) + \psi(B) \geq \frac{1}{2} \cdot \psi(A \Delta B).$$

Proof. By our hypothesis, it follows that $A \setminus B$, $B \setminus A$ and $A \cap B$ all have size $|A|/2$. Define u, v, w to be the vectors in \mathbb{R}^Ω defined by

$$\begin{aligned} u(\omega) &= \left(\prod_{z \in A \setminus B} P_z(\omega) \right)^{1/|A|}, \\ v(\omega) &= \left(\prod_{z \in B \setminus A} P_z(\omega) \right)^{1/|A|}, \\ w(\omega) &= \left(\prod_{z \in A \cap B} P_z(\omega) \right)^{1/|A|}. \end{aligned}$$

By the definition of Hellinger volume,

$$\begin{aligned} \psi(A) &= 1 - u \cdot w, \\ \psi(B) &= 1 - v \cdot w, \\ \psi(A \Delta B) &= 1 - u \cdot v. \end{aligned}$$

Thus the desired inequality is

$$2 - (u + v) \cdot w \geq (1 - u \cdot v)/2,$$

which is equivalent to

$$3 + u \cdot v \geq 2(u + v) \cdot w. \quad (1)$$

Since

$$\begin{aligned} \psi(A \setminus B) &= 1 - u \cdot u, \\ \psi(B \setminus A) &= 1 - v \cdot v, \\ \psi(A \cap B) &= 1 - w \cdot w, \end{aligned}$$

it follows that $\|u\|, \|v\|$ and $\|w\|$ are all at most 1. Thus $2(u + v) \cdot w \leq 2\|u + v\|$, and so (1) follows from

$$3 + u \cdot v \geq 2\|u + v\|.$$

Squaring both sides, it suffices to show

$$9 + 6u \cdot v + (u \cdot v)^2 \geq 4(\|u\|^2 + \|v\|^2 + 2u \cdot v)$$

Using the fact that $\|u\| \leq 1$ and $\|v\| \leq 1$ this reduces to

$$(1 - u \cdot v)^2 \geq 0,$$

which holds for all u, v . □

Let s_l, s_r be two disjoint subsets of $[k]$. Let $I_l \subseteq I$ (resp., I_r) be the set of strings with odd number of zeros in the coordinates indexed by s_l (resp., s_r). Let $s_p = s_l \cup s_r$ and $I_p = I_l \Delta I_r$. It is not hard to see that I_p is the set of strings with odd number of zeros in the coordinates indexed by s_p . By the symmetric-difference lemma,

$$\psi(I_l) + \psi(I_r) \geq \frac{\psi(I_p)}{2}. \quad (2)$$

For each $j \in [k]$, let $I_j \subseteq I$ be the set of strings where the j -th coordinate is set to zero. Applying the above observation inductively, we can obtain the following lemma.

Lemma 5. *Let $s \subseteq [k]$ be an arbitrary non-empty set and let $I_s \subseteq I$ be the set of strings with odd number of zeros in the coordinates indexed by s . Then,*

$$\sum_{j \in s} \psi(I_j) \geq \frac{\psi(I_s)}{2^{\lceil \log |s| \rceil}}.$$

Proof. We prove the claim via induction on the size of s . If s is a singleton set, it trivially holds. Otherwise, assume that for any subset of $[k]$ of size less than $|s|$, the claim is true.

Partition s into two non-empty subsets s_l, s_r with the property that $|s_l| = \lceil |s|/2 \rceil$ and $|s_r| = \lfloor |s|/2 \rfloor$. Then $\lceil \log |s| \rceil = 1 + \max\{\lceil \log |s_l| \rceil, \lceil \log |s_r| \rceil\}$. By the inductive hypothesis,

$$\sum_{j \in s_l} \psi(I_{s_l}) \geq \frac{\psi(I_{s_l})}{2^{\lceil \log |s_l| \rceil}} \quad \text{and} \quad \sum_{j \in s_r} \psi(I_{s_r}) \geq \frac{\psi(I_{s_r})}{2^{\lceil \log |s_r| \rceil}}.$$

Thus,

$$\begin{aligned}
\sum_{j \in s} \psi(I_{s_l}) &= \sum_{j \in s_l} \psi(I_{s_l}) + \sum_{j \in s_r} \psi(I_{s_r}) \\
&\geq \frac{\psi(I_{s_l})}{2^{\lceil \log |s_l| \rceil}} + \frac{\psi(I_{s_r})}{2^{\lceil \log |s_r| \rceil}} && \text{by the Inductive Hypothesis,} \\
&\geq \frac{1}{2^{\lceil \log |s| \rceil - 1}} [\psi(I_{s_l}) + \psi(I_{s_r})] && \text{by the choice of } s_l \text{ and } s_r, \\
&\geq \frac{1}{2^{\lceil \log |s| \rceil}} \psi(I_s) && \text{by Equation (2).}
\end{aligned}$$

□

Let $I_{OZ} \subseteq I$ be the set of strings which have odd number of zeros. The next corollary is an immediate consequence of Lemma 5 when $s = [k]$.

Lemma 6.

$$\sum_{j=1}^k \psi(I_j) \geq \frac{\psi(I_{OZ})}{2^{\lceil \log k \rceil}}.$$

NOF communication complexity and Hellinger volume It was shown in [BYJKS04] that the distribution of transcripts of a two-party protocol on a fixed input is a product distribution. The same is true for a multi-party NOF protocol.

Lemma 7. *Let Π be a k -player NOF communication protocol with input set $\mathcal{Z} = \mathcal{Z}_1 \times \dots \times \mathcal{Z}_k$ and let Ω be the set of possible transcripts. For each $j \in [k]$, there is a mapping $q_j : \Omega \times \mathcal{Z}^{-j} \rightarrow \mathbb{R}$, such that for every $z = (z_1, \dots, z_k) \in \mathcal{Z}$ and $\omega \in \Omega$,*

$$\Pr[\Pi(z) = \omega] = \prod_{j=1}^k q_j(\omega; z^{-j}).$$

Proof. Suppose $|\Pi(z)| \leq l$. For $i = 1, \dots, l$, let $\Pi_i(z)$ denote the i -th bit sent in an execution of the protocol. Let $\sigma_i \in [k]$ denote the player that sent the i -th bit. Then

$$\begin{aligned}
\Pr[\Pi(z) = \omega] &= \Pr[\Pi_1(z) = \omega_1, \dots, \Pi_l(z) = \omega_l] \\
&= \prod_{i=1}^l \Pr[\Pi_i(z) = \omega_i | \Pi_{<i}(z) = \omega_{<i}], \\
&= \prod_{i=1}^l \Pr[\Pi_i(z^{-\sigma_i}; \omega_{<i}) = \omega_i],
\end{aligned}$$

because every bit sent by player j depends only on z^{-j} and the transcript up to that point. We set

$$q_j(\omega; z^{-j}) = \prod_{i: \sigma_i = j} \Pr[\Pi_i(z^{-j}; \omega_{<i}) = \omega_i]$$

to obtain the expression of the lemma. □

As a corollary, we have the following cut-and-paste property for Hellinger volume.

Lemma 8. *Let $I_{OZ} \subseteq I$ be the set of inputs which have odd number of zeros, and let $I_{EZ} = I \setminus I_{OZ}$. Then*

$$\psi(I_{OZ}) = \psi(I_{EZ}).$$

Proof. Using the expression of the previous lemma, we have that for any $\omega \in \Omega$,

$$\prod_{v \in I_{OZ}} P_v(\omega) = \prod_{v \in I_{OZ}} \prod_{j=1}^k q_j(\omega; v^{-j}) = \prod_{u \in I_{EZ}} \prod_{j=1}^k q_j(\omega; u^{-j}) = \prod_{u \in I_{EZ}} P_u(\omega).$$

The middle equality holds, because for each $j \in [k]$ and $v \in I_{OZ}$ there is a unique $u \in I_{EZ}$ such that $v^{-j} = u^{-j}$. \square

Lower bounding Hellinger volume Eventually, we will need to provide a lower bound for the Hellinger volume of several distributions over protocol transcripts. In the two-party case, one lower bounds the Hellinger distance between the distribution of the transcripts on an accepting input and the distribution of the transcripts on a rejecting input. The following lemma will allow for similar conclusions in the multi-party case.

Lemma 9. *Let $A \subseteq I$ be of size $t \geq 2$. Suppose there is an event $T \subseteq \Omega$, a constant $0 \leq \delta \leq 1$ and an element v in A such that $P_v(T) \geq 1 - \delta$ and that for all $u \in A$ with $u \neq v$, $P_u(T) \leq \delta$. Then*

$$\psi(A) \geq (2 - 4\sqrt{\delta(1-\delta)}) \cdot \frac{1}{t}.$$

Proof. We need to show

$$1 - \sum_{\omega \in \Omega} \prod_{u \in A} P_u(\omega)^{\frac{1}{t}} \geq (2 - 4\sqrt{\delta(1-\delta)}) \cdot \frac{1}{t}.$$

Let $a = P_v(T) = \sum_{\omega \in T} P_v(\omega)$ and $b = \sum_{\omega \in T} \frac{1}{t-1} \sum_{u \neq v} P_u(\omega)$. Notice that by assumption $a \geq 1 - \delta$ and $b \leq \delta$.

Recall Hölder's inequality: for any nonnegative $x_k, y_k, k \in m$,

$$\sum_{k=1}^m x_k y_k \leq \left(\sum_{k=1}^m x_k^t \right)^{\frac{1}{t}} \left(\sum_{k=1}^m y_k^{\frac{t}{t-1}} \right)^{\frac{t-1}{t}}.$$

We first treat the sum over $\omega \in T$.

$$\begin{aligned} \sum_{\omega \in T} \prod_{u \in A} P_u(\omega)^{\frac{1}{t}} &= \sum_{\omega \in T} P_v(\omega)^{\frac{1}{t}} \prod_{u \neq v} P_u(\omega)^{\frac{1}{t}} \\ &\leq \left(\sum_{\omega \in T} P_v(\omega) \right)^{\frac{1}{t}} \left(\sum_{\omega \in T} \prod_{u \neq v} P_u(\omega)^{\frac{1}{t-1}} \right)^{\frac{t-1}{t}} \\ &\leq \left(\sum_{\omega \in T} P_v(\omega) \right)^{\frac{1}{t}} \left(\sum_{\omega \in T} \frac{1}{t-1} \sum_{u \neq v} P_u(\omega) \right)^{\frac{t-1}{t}} \\ &= a^{\frac{1}{t}} b^{\frac{t-1}{t}}, \end{aligned}$$

where we first used Hölder's inequality and then the arithmetic-geometric mean inequality. We do the same steps for the sum over $\omega \notin T$ to find

$$\sum_{\omega \notin T} \prod_{u \in A} P_u(\omega)^{\frac{1}{t}} \leq (1-a)^{\frac{1}{t}} (1-b)^{\frac{t-1}{t}}.$$

Hence,

$$\sum_{\omega \in \Omega} \prod_{u \in A} P_u(\omega)^{\frac{1}{t}} \leq a^{\frac{1}{t}} b^{\frac{t-1}{t}} + (1-a)^{\frac{1}{t}} (1-b)^{\frac{t-1}{t}}.$$

Let $g(a, b, x) = a^x b^{1-x} + (1-a)^x (1-b)^{1-x}$. We will show that under the constraints $a \geq 1 - \delta$ and $b \leq \delta$ where $\delta < 1/2$, for any fixed $0 \leq x \leq 1/2$, $g(a, b, x)$ is maximized for $a = 1 - \delta$ and $b = \delta$. The partial derivatives for $g(a, b, x)$ with respect to a and b are

$$g_a(a, b, x) = x[a^{x-1}b^{1-x} - (1-a)^{x-1}(1-b)^{1-x}] = x\left[\left(\frac{b}{a}\right)^{1-x} - \left(\frac{1-b}{1-a}\right)^{1-x}\right]$$

$$g_b(a, b, x) = (1-x)[a^x b^{-x} - (1-a)^x (1-b)^{-x}] = (1-x)\left[\left(\frac{b}{a}\right)^{-x} - \left(\frac{1-b}{1-a}\right)^{-x}\right]$$

Under our constraints, $\frac{b}{a} < 1 < \frac{1-b}{1-a}$, $1-x > 0$ and $-x \leq 0$, thus, $g_a(a, b, x) < 0$ and $g_b(a, b, x) \geq 0$ for any such a, b , and x . This implies that for any fixed b , $g(a, b, x)$ is maximized when $a = 1 - \delta$ and similarly for any fixed a , $g(a, b, x)$ is maximized when $b = \delta$. Therefore, for all a, b , and $0 \leq x \leq 1$, $g(a, b, x) \leq g(1 - \delta, \delta, x)$.

For $0 \leq x \leq 1/2$, let

$$f(\delta, x) = 1 - g(1 - \delta, \delta, x) = 1 - (1 - \delta)^x \delta^{1-x} - \delta^x (1 - \delta)^{1-x}.$$

Since $f(\delta, x)$ is convex for any constant $0 \leq \delta \leq 1$,

$$f(\delta, x) \geq \frac{f(\delta, 1/2) - f(\delta, 0)}{1/2 - 0} \cdot x = 2(1 - 2\sqrt{\delta(1 - \delta)}) \cdot x.$$

□

5 An application

In this section we show how to derive a lower bound for the informational complexity of the AND_k function. Define a collection of distributions $\eta = \{\zeta_1, \dots, \zeta_k\}$, where, for each $j \in [k]$, ζ_j is the uniform distribution over I_j . Recall that $I_j \subseteq I = \{0, 1\}^k$ for $j \in [k]$ is the set of k -bitstrings whose j -th bit is 0. We prove the following lower bound on the δ -error informational complexity of AND_k with respect to η .

Remark. The choice of the collection η is not arbitrary, but is suggested by the way the direct-sum theorem for informational complexity is proved in [BYJKS04] for the two-party setting. In particular, two properties of η seem crucial for such a purpose. First, for each $j \in [k]$, ζ_j is a distribution with support only on the zeroes of AND_k . Second, under any ζ_j , the input of each player is independent of any other input.

Theorem 10.

$$\text{IC}_{\eta, \delta}(\text{AND}_k) \geq \log e \cdot (1 - 2\sqrt{\delta(1 - \delta)}) \cdot \frac{1}{k^2 4^{k-1}}.$$

Proof. Let Π be a δ -error protocol for AND_k . By Lemma 3 we have that,

$$I(Z; \Pi(Z)) \geq \frac{1}{2^{k-1} \ln 2} \cdot \psi(I_j),$$

where $Z \sim \zeta_j$, for any $j \in [k]$, Thus, by the definition of $\text{IC}_{\eta,\delta}(\text{AND}_k)$,

$$\text{IC}_{\eta,\delta}(\text{AND}_k) \geq \sum_{j=1}^k \frac{1}{k 2^{k-1} \ln 2} \cdot \psi(I_j).$$

Applying in turn Lemmas 6, 8, and 9 we have

$$\text{IC}_{\eta,\delta}(\text{AND}_k) > \frac{\psi(I_{OZ})}{k^2 2^k \ln 2} = \frac{\psi(I_{EZ})}{k^2 2^k \ln 2} \geq \log e \cdot (1 - 2\sqrt{\delta(1-\delta)}) \cdot \frac{1}{k^2 4^{k-1}},$$

where the application of Lemma 9 is with $A = I_{EZ}$, $t = 2^{k-1}$, T the set of transcripts that output “1”, and v the all-one vector in I . \square

It is of interest to note, that

$$\text{IC}_{\eta,\delta}(\text{AND}_k) \leq \frac{1}{k} \cdot H(1/2^{k-1}) = O(1/2^k).$$

This is achieved by the following protocol. The players, one by one, reveal with one bit whether they see a 0 or not. The communication ends with the first player that sees a 0. The amount of information revealed is $H(1/2^{k-1})$ under ζ_1 and 0 otherwise.

6 Difficulties in proving a direct-sum theorem

There seem to be fundamental difficulties in proving a direct-sum theorem on informational complexity in the NOF model. The reader familiar with the techniques of Bar-Yossef, Jayram, Kumar & Sivakumar [BYJKS04], should recall that in the first part of the method a direct-sum for informational complexity of disjointness is proved. In particular, it is shown that with respect to suitable collections of distributions η and ζ for $\text{DISJ}_{n,2}$ and AND_2 respectively, the information cost of $\text{DISJ}_{n,2}$ is at least n times the informational complexity of AND_2 : $\text{IC}_{\eta,\delta}(\text{DISJ}_{n,2}) \geq n \cdot \text{IC}_{\zeta,\delta}(\text{AND}_2)$. This is achieved via a simulation argument in which the players, to decide the AND_2 function, use a protocol for disjointness by substituting their inputs in a special copy of AND_2 and using their random bits to generate the inputs for the rest $n-1$ copies of AND_2 . In the NOF model the players can no longer perform such a simulation. This is because, with private random bits, they cannot agree on what the input on the rest of the copies should be without additional communication. This problem can be overcome if we think of their random bits as being not private, but on each player’s forehead, just like the input. However, In such a case, although the direct-sum theorem holds, it is useless. This is because $\text{IC}_{\zeta,\delta}(\text{AND}_k) = 0$, as is shown by the protocol we describe in the next paragraph.

We describe a protocol that computes AND_k on every input, with one-sided error. It has the property that for any distribution over the zeroes of AND_k , no player learns anything about his own input. We give the details for three players. Let x_1, x_2, x_3 denote the input. Each player has two random bits on his forehead, denoted a_1, a_2, a_3 and b_1, b_2, b_3 . The first player does the following: if $x_2 = x_3 = 1$, he sends $a_2 \oplus a_3$, otherwise he sends $a_2 \oplus b_3$. The other two players behave analogously. If the XOR of the three messages is ‘0’, they answer ‘1’, otherwise they know that the answer is ‘0’. Notice that any player learns nothing from another player’s message. This is because the one-bit message is XOR-ed with one of his own random bits, which he cannot see.

References

- [Abl96] Farid M. Ablayev. Lower bounds for one-way probabilistic communication complexity and their application to space complexity. *Theor. Comput. Sci.*, 157(2):139–159, 1996.
- [BHHR14] Beame, Hopkins, Hrubes, and Rashtchian. Paul Beame, personal communication, 2014.
- [BHN09] Paul Beame and Dang-Trinh Huynh-Ngoc. Multiparty communication complexity and threshold circuit size of AC^0 . In *FOCS*, pages 53–62. IEEE Computer Society, 2009.
- [BNS92] László Babai, Noam Nisan, and Mario Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *J. Comput. Syst. Sci.*, 45(2):204–232, 1992.
- [BPS05] Paul Beame, Toniann Pitassi, and Nathan Segerlind. Lower bounds for Lovász-Schrijver systems and beyond follow from multiparty communication complexity. In *In Proc. 32nd Int. Conf. on Automata, Languages and Programming (ICALP’05)*, pages 1176–1188, 2005.
- [BT94] Richard Beigel and Jun Tarui. On acc. *Computational Complexity*, 4:350–366, 1994.
- [BYJKS02] Ziv Bar-Yossef, T. S. Jayram, Ravi Kumar, and D. Sivakumar. Information theory methods in communication complexity. In *IEEE Conference on Computational Complexity*, pages 93–102, 2002.
- [BYJKS04] Ziv Bar-Yossef, T. S. Jayram, Ravi Kumar, and D. Sivakumar. An information statistics approach to data stream and communication complexity. *J. Comput. Syst. Sci.*, 68(4):702–732, 2004.
- [CA08] A. Chattopadhyay and A. Ada. Multiparty communication complexity of disjointness. Technical Report TR-08-002, ECCC, 2008.
- [CFL83] Ashok K. Chandra, Merrick L. Furst, and Richard J. Lipton. Multiparty protocols. In *Proceedings of the fifteenth annual ACM symposium on Theory of computing*, STOC ’83, pages 94–99, New York, NY, USA, 1983. ACM.
- [CKS03] Amit Chakrabarti, Subhash Khot, and Xiaodong Sun. Near-optimal lower bounds on the multi-party communication complexity of set disjointness. In *IEEE Conference on Computational Complexity*, pages 107–117. IEEE Computer Society, 2003.
- [CSWY01] Amit Chakrabarti, Yaoyun Shi, Anthony Wirth, and Andrew Yao. Informational complexity and the direct sum problem for simultaneous message complexity. In *In Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, pages 270–278, 2001.
- [CT93] Fan R. K. Chung and Prasad Tetali. Communication complexity and quasi randomness. *SIAM J. Discrete Math.*, 6(1):110–123, 1993.

- [CT06] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley-Interscience, 2006.
- [FG05] Jeff Ford and Anna Gál. Hadamard tensors and lower bounds on multi-party communication complexity. In *In ICALP*, pages 1163–1175, 2005.
- [Gro94] Vince Grolmusz. The BNS lower bound for multi-party protocols in nearly optimal. *Inf. Comput.*, 112(1):51–54, 1994.
- [HG90] Johan Håstad and Mikael Goldmann. On the power of small-depth threshold circuits. In *FOCS*, volume II, pages 610–618. IEEE, 1990.
- [Jay09] T. S. Jayram. Hellinger strikes back: A note on the multi-party information complexity of and. In *Proceedings of the 12th International Workshop and 13th International Workshop on Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX '09 / RANDOM '09*, pages 562–573, Berlin, Heidelberg, 2009. Springer-Verlag.
- [JKS03] T. S. Jayram, Ravi Kumar, and D. Sivakumar. Two applications of information complexity. In *STOC*, pages 673–682. ACM, 2003.
- [Kla07] Hartmut Klauck. Lower bounds for quantum communication complexity. *SIAM Journal of Computation*, 37(1), 2007.
- [KN06] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, New York, NY, USA, 2006.
- [LS07] Nati Linial and Adi Shraibman. Lower bounds in communication complexity based on factorization norms. In *Proceedings of the 39th Symposium on the Theory of Computation*, pages 699–708. ACM, 2007.
- [LS09] Troy Lee and Adi Shraibman. Disjointness is hard in the multiparty number-on-the-forehead model. *Computational Complexity*, 18(2):309–336, 2009.
- [Lue03] D.G. Luenberger. *Linear and nonlinear programming*. Kluwer Academic, 2003.
- [Nis94] Noam Nisan. The communication complexity of threshold gates. In *Proceedings of “Combinatorics, Paul Erdos is Eighty”*, pages 301–315, 1994.
- [NW91] Noam Nisan and Avi Wigderson. Rounds in communication complexity revisited. In *STOC*, pages 419–429. ACM, 1991.
- [Raz00] Ran Raz. The bns-chung criterion for multi-party communication complexity. *Computational Complexity*, 9(2):113–122, 2000.
- [Raz03] Alexander Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya: Mathematics*, 67(1):145–159, 2003.
- [RY14] Anup Rao and Amir Yehudayoff. <http://eccc.hpi-web.de/report/2014/060/>, 2014.

- [She11] Alexander Sherstov. The pattern matrix method. *SIAM Journal on Computing*, 40(6):1969–2000, 2011.
- [She12] Alexander A. Sherstov. The multiparty communication complexity of set disjointness. In Howard J. Karloff and Toniann Pitassi, editors, *STOC*, pages 525–548. ACM, 2012.
- [She13] Alexander A. Sherstov. Communication lower bounds using directional derivatives. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *STOC*, pages 921–930. ACM, 2013.
- [SS02] Michael Saks and Xiaodong Sun. Space lower bounds for distance approximation in the data stream model. In *STOC '02: Proceedings of the thirty-fourth annual ACM symposium on Theory of computing*, pages 360–369, New York, NY, USA, 2002. ACM.